VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts IP 4537 PCT	**WEITERES VORGEHEN** siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP 03/08024	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 23.07.2003	Prioritätsdatum *(Tag/Monat/Jahr)* 21.08.2002
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G06F1/00		
Anmelder AUDI AG		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 11 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Bescheids
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Regel 66.2 a)ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 17.03.2004	Datum der Fertigstellung dieses Berichts 20.12.2004
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Bevollmächtigter Bediensteter Sigolo, A Tel. +31 70 340-4173

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP 03/08024

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung *(Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17))*:

Beschreibung, Seiten

1-9 eingegangen am 15.11.2004 mit Schreiben vom 12.11.2004

Ansprüche, Nr.

1-8 eingegangen am 15.11.2004 mit Schreiben vom 12.11.2004

Zeichnungen, Blätter

1/4-4/4 in der ursprünglich eingereichten Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um:

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).

   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:

   ☐ Ansprüche, Nr.:

   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen.)

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-8
	Nein:	Ansprüche	
Erfinderische Tätigkeit (IS)	Ja:	Ansprüche	
	Nein:	Ansprüche	1-8
Gewerbliche Anwendbarkeit (IA)	Ja:	Ansprüche:	1-8
	Nein:	Ansprüche:	

2. Unterlagen und Erklärungen:

   siehe Beiblatt

Zu Punkt V

Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Es wird auf das folgende Dokument verwiesen:
D1: EP-A-1 197 826 (TOKYO SHIBAURA ELECTRIC CO) 17. April 2002 (2002-04-17)

1. Die vorliegende Anmeldung erfüllt nicht die Erfordernisse des Artikels 33(1) PCT, weil der Gegenstand des Anspruchs 1 nicht auf einer erfinderischen Tätigkeit im Sinne von Artikel 33(3) beruht.

1.1 Die angegebene technische Aufgabe der vorliegenden Anmeldung ist es, ein Fahrzeug-Steuergerät zu schaffen, bei dem ein Austausch eines Speicherbausteins und die Änderung der Daten sowie des Codes auf dem Speicherbaustein nicht möglich ist, ohne die Funktionsfähigkeit des Fahrzeug-Steuergeräts zu beeinflussen (siehe Beschreibung: Seite 1, letzen Absatz - Seite 2, ersten Absatz).

1.2 Die Tatsache, dass es sich um ein Fahrzeug-Steuergerät handelt, kann aber nicht als besonderes technisches Merkmal angesehen werden, trägt nicht zur Lösung der obengenannten Aufgabe bei und engt deshalb in keiner Weise den technischen Anwendungsbereich ein.

1.3 Um den nächstliegenden Stand der Technik zu beurteilen, würde der Fachmann deshalb alle Dokumente berücksichtigen, die die Sicherung elektronischer Geräte gegen unerlaubte Manipulation der Speicherbausteine behandeln.

1.4 D1 offenbart ein Verfahren zum Schutz eines solchen Geräts, hier in Form einer tragbaren Speicherkarte. Aufgabe der Erfindung von D1 ist es, ein Verfahren zum Schutz vor Manipulation an einem solchen Gerät zu schaffen, bei dem unerwünschte Veränderungen der Speicherbausteine verhindert werden. Beispielweise ist es nicht möglich, nicht einmal für den Besitzer, einen Speicherbaustein auszutauschen, ohne die Funktionsfähigkeit des Geräts zu beeinflussen. Dazu werden zum Beispiel zwei Kennungen miteinander verglichen. Außerdem werden zuerst die Daten, die später auf einem reversiblen Speicherbaustein abgelegt werden, durch ein Verschlüsselungsverfahren, das eine bausteinspezifische Kennung eines zweiten

Bausteins des Geräts als Schlüssel verwendet, verschlüsselt.

D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 1 angesehen.

1.5 Insbesondere offenbart D1 (die Verweise in Klammern beziehen sich auf dieses Dokument) ein gesichertes elektronisches Gerät (siehe Spalte 1, Zeilen 18-24), das einen Microrechner und einen Speicherbaustein umfasst (siehe Spalte 3, Zeilen 42-45; Spalte 4, Zeilen 16-19; Abbildung 17), wobei der Speicherbaustein eine spezifische Kennung aufweist ("memory 4 is certified by use of the *certification key* ... unalterably stored in the memory 4") und der Mikrorechner einen Bereich aufweist, in dem diese spezifische Kennung des Speicherbausteins abgelegt ist ("*certification key* unalterably stored in the internal memory 3b", siehe das erste Ausführungsbeispiel, Spalte 4, Zeilen 26-38).

1.6 Der Gegenstand des Anspruchs 1 unterscheidet sich daher von dem bekannten D1 dadurch, daß es in der vorliegenden Anmeldung um ein Fahrzeug-Steuergerät handelt. Dieses Merkmal kann aber nicht als besonderes technisches Merkmal angesehen werden, trägt nicht zur Lösung der obengenannten Aufgabe bei und engt deshalb in keiner Weise den technischen Anwendungsbereich ein. Deshalb beruht Anspruch 1 nicht auf einer erfinderischen Tätigkeit im Sinne von Artikel 33(3).

2. Die abhängigen Ansprüche 2 zu 8 enthalten keine Merkmale, die in Kombination mit den Merkmalen irgendeines Anspruchs, auf den sie sich beziehen, die Erfordernisse des PCT in bezug auf erfinderische Tätigkeit erfüllen.

2.1 **Ansprüche 2, 3 und 4.** Der Gegenstand der Ansprüche 2, 3 und 4 ist ebenfalls aus D1 bekannt, da der Mikrorechner-Bereich (ROM memory portion), in dem die Kennung des Speicherbausteins abgelegt ist, nur einmalig beschreibbar ist, das Gerät eine Authentifizierungseinheit zur Authentifizierung des mit dem Mikrorechner verbundenen Speicherbausteins aufweist und die Authentifizierungseinheit durch ein Programm gebilded wird, das dem vergleich der Kennungen dient.

2.2 **Anspruch 5.** Der Gegenstand des Anspruchs 5 ist auch aus D1 bekannt, weil die Authentifizierungseinheit durch ein Programm gebilded wird, das der Verschlüsselung von Daten dient, wobei das Programm auf eine in dem Mikrorechner gespeicherte Kennung zugreift (siehe drittes und viertes Ausführungsbeispiel: Spalte 7,

Zeilen 34-41 und 49-53; Spalte 8, Zeilen 30-41; Abbildungen 14, 17).

2.3 **Ansprüche 6, 7 und 8.** Ansprüche 6, 7 und 8 beschreiben nur Merkmale, die der Fachmann als eine übliche, konstruktive Maßnahme zur Lösung der gestellten Aufgabe ansehen würde.

IP 4537
Pz

Fahrzeug-Steuergerät

Beschreibung

Die vorliegende Erfindung betrifft ein vor Manipulationen geschütztes Fahrzeug-Steuergerät, gemäß dem Oberbegriff des Patentanspruchs 1.

In Kraftfahrzeugen werden heutzutage zur Steuerung einzelner Kfz-Komponenten Steuergeräte verwendet, wie beispielsweise das Motorsteuergerät oder das Getriebesteuergerät. Die zum Betrieb von solchen Steuergeräten erforderlichen Informationen, wie beispielsweise Programme und Daten, werden verschlüsselt oder unverschlüsselt in Speicherbausteinen (E^2PROM, Flash und dergleichen) abgelegt. Das Verschlüsselungsverfahren ist dabei unabhängig von einer festen Hardware-Kombination von Bausteinen und in der Regel in einem wiederbeschreibbaren Speichermedium abgelegt.

Der Nachteil solcher Steuergeräte und der verwendeten Programme besteht darin, dass einzelne Speicherbausteine ausgetauscht werden können, bzw. die Daten auf den Speicherbausteinen über eine Diagnoseschnittstelle oder über direkten Zugriff auf den Speicherbaustein überschrieben werden können. Der Austausch eines Speicherbausteins oder das Überschreiben der auf diesem Speicherbaustein gespeicherten Daten und Programme kann dazu führen, dass die Kfz-Komponente mit anderen Kenndaten arbeitet. Dies wird beispielsweise bei dem sogenannten Chip-Tuning durchgeführt, bei dem Speicherbausteine, die dem Motorsteuergerät zugeordnet sind, ausgetauscht bzw. die auf diesen Speicherbausteinen gespeicherten Programme und Daten, wie Kenndaten, geändert werden. Dadurch kann beispielsweise eine Erhöhung der Leistung und/oder des Drehmoments des Motors erzielt werden. Wird diese Manipulation durchgeführt ohne die weiteren Kfz-Komponenten, wie Ölkühler, Turbolader oder Bremsen anzupassen, so kann es zu Schäden an diesen Kfz-Komponenten und sicherheitskritischen Zuständen kommen.

Aufgabe der vorliegenden Erfindung ist es daher, ein Fahrzeug-Steuergerät zu schaffen, bei dem ein Austausch eines Speicherbausteins und die Ände-

rung der Daten sowie des Codes auf dem Speicherbaustein nicht möglich ist, ohne die Funktionsfähigkeit des Steuergeräts zu beeinflussen oder zumindest die Veränderung zu diagnostizieren und diese ggf. zur Anzeige zu bringen.

Der Erfindung liegt die Erkenntnis zugrunde, dass diese Aufgabe gelöst werden kann, indem eine Kennung der ursprünglichen Speicherbausteine eines Steuergeräts, die nicht verändert werden kann, als Identifikationsmittel verwendet wird.

Die Aufgabe der Erfindung wird dadurch gelöst, das bei einem Fahrzeug-Steuergerät der Mikrorechner zumindest eine spezifische Kennung des ursprüngliche Speicherbausteins von dem Speicherbaustein ausliest und speichert.

Durch Sicherung der spezifischen Kennung des ursprünglichen Speicherbausteins wird eine Konstante gegeben, die zur Erkennung des Austauschs eines Speicherbausteins oder der Manipulation von Daten dienen kann. Die Kennung kann eine Identifikationsnummer des Speicherbausteins darstellen. Es ist aber auch möglich, als Kennung Daten, die zu einem bestimmten Zeitpunkt aufgenommen wurden, in Form eines Fingerprints zu verwenden. Schließlich kann die Kennung weitere Informationen, wie beispielsweise das Herstellungsdatum bzw. das Datum der ersten Inbetriebnahme des Steuergeräts beinhalten.

Vorzugsweise wird die mindestens eine Kennung in einem nur einmalig beschreibbaren OTP (one-time-programmable)-Bereich des Mikrorechners abgelegt. Dadurch kann eine Modifikation der Kennung in dem Mikrorechner verhindert werden und so der Schutz vor Manipulationen erhöht werden.

Die in dem Mikrorechner gespeicherten Kennungen werden in dem erfindungsgemäßen Verfahren zumindest teilweise zur Authentifizierung von Speicherbausteinen verwendet. Bei jedem Hochfahren des Steuergeräts können anhand der ursprünglichen Kennungen, die in dem Mikrorechner abgelegt sind, die tatsächlich mit dem Mikrorechner verbundenen Speicherbausteine einer Authentifizierung unterzogen werden.

In einer Ausführungsform kann die Authentifizierung der Speicherbausteine durch Vergleich der im Mikrorechner gespeicherten Kennung der ursprüngli-

chen Speicherbausteine mit der Kennung der aktuellen Speicherbausteine erfolgen. Hierbei werden bei der Inbetriebnahme des Steuergeräts von dem Mikrorechner die aktuellen Kennungen der mit dem Mikrorechner verbundenen aktuellen Speicherbausteine ausgelesen und mit den ursprünglichen Kennungen, die in dem Mikrorechner abgelegt sind, verglichen. Dadurch kann ein Austausch eines oder mehrerer der Speicherbausteine erkannt und Maßnahmen durchgeführt werden, beispielsweise kann eine Betätigung des Steuergeräts durch den Mikrorechner verhindert werden.

Alternativ oder zusätzlich kann eine Authentifizierung der Speicherbausteine durch Verschlüsselung von Daten oder Programmen erfolgen, wobei der Schlüssel mindestens einen Teil einer der ursprünglichen Kennungen beinhaltet. Dadurch kann erzielt werden, dass bei Abweichung der Kennung von einer ursprünglichen Kennung der Mikrorechner nicht auf Daten oder Programme zugreifen kann und das Steuergerät damit nicht lauffähig ist.

Die unverschlüsselt oder verschlüsselt auf zumindest einem der Speicherbausteine abgelegten Daten oder Programme können in Form eines Fingerprints dargestellt werden, der die Daten und Programme zu einem gewissen Zeitpunkt festhält. Werden die Daten oder Programme geändert, so kann bei der erneuten Erfassung des Fingerprints durch Vergleich mit dem verschlüsselt abgelegten Fingerprint eine Manipulation erkannt werden.

Gemäß einem zweiten Aspekt der Erfindung wird die Aufgabe gelöst durch ein Steuergerät für eine Kfz-Komponente, das zumindest einen Mikrorechner (μC) und zumindest einen Speicherbaustein umfasst, wobei der mindestens eine Speicherbaustein zumindest eine spezifische Kennung aufweist und der Mikrorechner zumindest einen Bereich aufweist, in dem die mindestens eine spezifische, ursprüngliche Kennung abgelegt ist.

Um die Manipulation durch Veränderung der in dem Mikrorechner abgelegten Kennung zu verhindern, kann der Mikrorechner einen Bereich, der nur einmalig beschreibbar ist (OTP-Bereich), aufweisen und die spezifische, ursprüngliche Kennung des mindestens einen Speicherbausteins in diesem Bereich abgelegt sein. Dieser OTP-Bereich kann zusätzlich lesegeschützt ausgestaltet sein.

Das Steuergerät kann zusätzlich eine Authentifizierungseinheit zur Authentifizierung der mit dem Mikrorechner verbundenen Speicherbausteine aufwei-

sen, wobei diese ein Programm, das auf dem Mikrorechner abgelegt ist, darstellen kann.

Die Authentifizierungseinheit kann daher durch ein Programm gebildet werden, das auf dem Mikrorechner abgelegt ist und dem Vergleich der ursprünglichen Kennungen mit zumindest einer aktuellen Kennung zumindest eines Speicherbausteins dient. Alternativ oder zusätzlich kann das Programm zur Verschlüsselung von Daten oder Programmen auf mindestens eine der in dem Mikrorechner gespeicherten ursprünglichen Kennungen zugreifen.

Mindestens einer der Speicherbausteine des Steuergeräts kann in dem Mikrorechner integriert sein. Es kann sich dabei um einen embedded Flash-Speicher oder um eine E²PROM Emulation im embedded Flash Speicher handeln. . Auch in diesem Fall kann das Ablegen einer Kennung des Speicherbausteins in einem OTP-Bereich des Mikrorechners vorteilhaft genutzt werden. Analog zu externen Speichern kann eine Authentifizierung der Speicherbausteine durch Verschlüsselung von Daten oder Programmen erfolgen, wobei der Schlüssel mindestens einen Teil einer der ursprünglichen Kennungen beinhaltet. Dadurch kann erzielt werden, dass bei Abweichung der Kennung von einer ursprünglichen Kennung der Mikrorechner nicht auf Daten oder Programme zugreifen kann und das Steuergerät damit nicht lauffähig ist.

Merkmale und Details, die im Zusammenhang mit dem erfindungsgemäßen Verfahren beschrieben werden, gelten entsprechend für das erfindungsgemäße Steuergerät und umgekehrt.

Die Erfindung wird im Folgenden anhand der beiliegenden Zeichnungen, die sich auf mögliche Ausführungsbeispiele der Erfindung beziehen, beschrieben. Es zeigen:

Figur 1: eine schematische Blockdarstellung einer ersten Ausführungsform des erfindungsgemäßen Steuergeräts;

Figur 2: ein Flussdiagramm, das eine Ausführungsform des erfindungsgemäßen Verfahrens darstellt;

Figur 3: eine schematische Blockdarstellung einer zweiten Ausführungsform des erfindungsgemäßen Steuergeräts; und

Figur 4: eine schematische Blockdarstellung einer dritten Ausführungsform des erfindungsgemäßen Steuergeräts.

In Figur 1 ist eine Ausführungsform eines erfindungsgemäßen Steuergeräts dargestellt. Der Aufbau von Steuergeräten, wie beispielsweise Motorsteuergeräten, ist hinlänglich aus dem Stand der Technik bekannt, so dass hierauf nur insoweit eingegangen wird, wie dies für das Verständnis der Erfindung erforderlich ist. Das Steuergerät 1 umfasst in der dargestellten Ausführungsform einen Mikrorechner μC, einen Flash-Speicher 2 und einen EEPROM (E^2PROM) 3. Der Flash-Speicher 2 und der E^2PROM 3 weisen jeweils einen OTP-Bereich 21, 31 auf. Diese sind vorzugsweise nicht lesegeschützt ausgestaltet. Auch in dem μC ist ein OTP-Bereich 11 vorgesehen. Weiterhin ist in dem μC eine Authentifikationseinheit 12 enthalten. Diese kann eine elektronische Schaltung oder ein Programm in dem μC darstellen.

Die Speicherbausteine Flash 2, E^2PROM 3 sind in der dargestellten Ausführungsform mit bausteinindividuellen Identifikationsnummern ID versehen. Diese werden in der Regel beim Hersteller des Bausteins geschrieben und in den OTP-Bereich 21, 31 der einzelnen Bausteine abgelegt.

In Figur 2 ist ein Flussdiagramm gezeigt, das eine Ausführungsform des erfindungsgemäßen Verfahrens anhand der in Figur 1 gezeigten Ausführungsform des Steuergeräts darstellt.

Im Herstellungsprozess des Steuergeräts werden erfindungsgemäß bei der Erstinbetriebnahme des Steuergeräts von dem Mikrorechner μC die ID's der einzelnen Speicherbausteine 2, 3 ausgelesen und in einen einmalig beschreibbaren OTP-Bereich 11 des μC abgelegt. Ab diesem Zeitpunkt ist die Funktion des Steuergeräts 1 nur in Verbindung mit den dem μC bekannten ID's der externen Speicherbausteine 2, 3 möglich.

Bei jeder weiteren Inbetriebnahme des Steuergeräts 1 wird von dem μC die ID aller mit diesem verbundenen Speicherbausteine 2, 3 erneut ausgelesen. In einer Vergleichseinheit können dann diese aktuellen ID's mit den ursprünglichen Kennungen, die in dem OTP-Bereich 11 des μC abgelegt sind, verglichen werden. Wird bei diesem Vergleich festgestellt, dass eine der ID's

nicht mit einer der ursprünglichen ID's übereinstimmt, so wird das Steuergerät an seiner Funktion gehindert oder zumindest die Veränderung diagnostiziert und diese ggf. zur Anzeige gebracht

In Figur 3 ist eine weitere Ausführungsform des erfindungsgemäßen Steuergeräts 1 gezeigt. Der Aufbau ist im wesentlichen gleich dem Aufbau der Ausführungsform aus Figur 1, allerdings ist in dieser Ausführungsform der Code zum Betreiben des Steuergeräts in einen Master-Code (MC) und einen Sub-Code (SC) unterteilt. Der Mastercode MC enthält elementare, essentielle Funktionalitäten zum Betrieb des Steuergeräts, z.B. das Programm zur Signalerzeugung für angeschlossene Aktuatoren (nicht dargestellt) des Steuergeräts oder das Programm für die Berechnung der Stellgrößen und Stellwerte. Der Mastercode MC kann weiterhin Daten umfassen. In dem Sub-Code SC sind weitere Programme und Daten enthalten. Das Steuergerät ist nur funktionsfähig unter Verwendung beider Codes MC und SC. In der dargestellten Ausführungsform ist der Sub-Code SC in einem wiederbeschreibbaren Bereich des Flash-Speichers 2 enthalten. Der Master-Code MC ist in einem OTP-Bereich 11 des Mikrorechners μC enthalten. Der Master-Code ist vorzugsweise gegen Auslesen über die Kontaktierung geschützt. Dies kann beispielsweise physikalisch durch Durchlegieren einer Transistorstrecke oder schaltungstechnisch erzielt werden. Der Sub-Code SC kann im Gegesatz zu dem Master-Code MC modifiziert beziehungsweise überschrieben werden. Dies erlaubt ein Updaten des Subcodes oder ein Reprogrammieren.

Der μC weist weiterhin eine Identifikationsnummer μC-ID auf. Auch diese ist in einem lesegeschützten OTP-Bereich des μC abgelegt. In dem E^2PROM sind weitere Daten für den Betrieb des Steuergeräts in einem wiederbeschreibbaren Bereich abgelegt. Diese Daten können beispielsweise Adaptionswerte sowie Leerlaufdrehzahlen bei einem Motorsteuergerät, sein.

Beim Initialisieren des Steuergeräts lernt der Mikrorechner μC die in dem OTP-Bereich 21, 31 der Speicherbausteine 2, 3 abgelegten und dadurch nicht veränderbaren Identifikationsnummern an und legt diese in einem OTP-Bereich des Mikrorechners μC, der optional auch lesegeschützt ausgestaltet sein kann, ab.

Von diesem Zeitpunkt an sind dem Mikrorechner μC die mit diesem verbundenen Speicherbausteine 2, 3 über ihre ID bekannt.

Zusätzlich können die in dem Mikrorechner abgelegten ID's der Speicherbausteine auch zur Verschlüsselung von Daten oder Programmen dienen. So können die auf dem E²PROM abgelegten Daten beispielsweise durch ein symmetrisches Verschlüsselungsverfahren codiert werden, in dem der Schlüssel zumindest einen Teil der ID zumindest eines der Speicherbausteine 2, 3 umfasst. Bei einem Motorsteuergerät können in dem E²PROM beispielsweise Lernwerte, Fertigungsdaten, Anpassungswerte und dergleichen gespeichert sein. Zur Verschlüsselung sind grundsätzlich alle symmetrischen Verschlüsselungsverfahren geeignet, die die Einbeziehung eines steuergeräteindividuellen Kennzeichnens erlauben. Vorzugsweise werden die Daten des E²PROM durch einen Schlüssel verschlüsselt, der zusätzlich oder alternativ zu der ID der externen Speicherbausteine die ID des Mikrorechners μC umfasst. Hierdurch wird eine steuergeräteindividuelle Verschlüsselung erzielt, die ein Austauschen des E²PROMs oder ein Überschreiben der darauf gespeicherten Daten unmöglich macht bzw. den Betrieb des Steuergeräts nach einer solchen Manipulation verhindert. Der Schlüssel wird vorzugsweise in dem RAM-Speicher des Mikrorechners μC abgelegt. Dadurch wird der Schlüssel bei jedem Hochlaufen des Steuergeräts unter Einbeziehung eines steuergeräteindividuellen Kennzeichens (z.B. der ID des μC und gegebenenfalls der ID's der Speicherbausteine) gebildet und ist somit steuergeräteindividuell.

Weiterhin kann der Subcode SC auf dem Flash-Speicher 2 ganz oder teilweise verschlüsselt abgelegt sein. Auch für diese Verschlüsselung kann die ID der einzelnen Speicherbausteine oder des Mikrorechners bzw. ein Teil dieser ID in den Schlüssel integriert werden. Die Entschlüsselung der Daten in dem Sub-Code wird durch den Master-Code durchgeführt. Da dieser in einem lesegeschützten Bereich des Mikrorechners abgelegt ist, kann ein Auslesen des Programms und damit eine Vervielfältigung der Software verhindert werden.

Die Überwachung des Sub-Codes gegenüber Manipulation, die durch den μC im Master-Code sicher gestellt wird, kann auch über andere Verfahren als der Verschlüsselung erfolgen. So können zusätzlich oder alternativ lineare/CRC-Checksummenbildung oder Hash-Wertbildung verwendet werden. Zur Erkennung einer vorgenommenen Manipulation der Daten und gegebenenfalls Teile des Subcodes werden z.B. über ausgewählte Bereiche lineare Checksummen gebildet und das Ergebnis verschlüsselt als Fingerprint in den Sub-Code eingebracht. Der Mastercode berechnet im Steuergerätebetrieb,

beispielsweise bei einem Signal an Klemme 15, über den gleichen vordefinierten Bereich den Vergleichswert (z.B. lineare Checksumme) und prüft diesen gegen den entschlüsselten, im Sub-Code verschlüsselt abgelegten Referenzwert. Die Art der Manipulationserkennung kann beliebig gewählt werden.

Nach der Erkennung einer Manipulation werden vom Master-Code Maßnahmen eingeleitet, die gegebenenfalls zum Steuergeräteausfall führen.

In Figur 4 ist eine weitere Ausführungsform des erfindungsgemäßen Steuergeräts gezeigt. Bei dieser Ausführungsform sind die Speicherbausteine 2 und 3 in den Mikrorechner μC integriert. Der μC weist hierbei einen embedded Flash-Speicher auf, wobei der E²PROM emuliert wird. Diese Ausgestaltung des Steuergeräts weist zwar den Vorteil auf, dass ein Austausch der Speicherbausteine zuverlässig verhindert werden kann, allerdings sind die Daten bei der Emulation des E²PROM nur blockweise überschreibbar.

Das Verfahren zum Schutz gegen Manipulation erfolgt bei diesem Steuergerät mit internem Speicher im wesentlichen wie das oben für Steuergeräte mit externen Speichern beschriebene. Auch hierbei können insbesondere die Daten des emulierten E²PROM verschlüsselt abgelegt werden und durch einen Schlüssel, der zumindest eine individuelle Kennung des Steuergeräts, wie die μC-ID und/oder die Flash-ID umfasst, entschlüsselt werden. Ebenso können die in dem Subcode, der in dem Flash-Speicher des μC abgelegt ist, enthaltenen verschlüsselten Daten oder Fingerprints durch den Mastercode entschlüsselt werden. Auch hierbei wird vorzugsweise eine steuergeräteindividuelle Kennung in dem Schlüssel integriert.

Die Erfindung ist nicht auf die dargestellten Ausführungsformen beschränkt. So kann als Kennung der einzelnen Speicherbausteine beispielsweise das Herstellungdatum des Steuergeräts in Betracht kommen. Hierdurch kann eine Manipulation während der Garantiezeit verhindert werden.

Weiterhin ist es beispielsweise auch möglich, den zum Betrieb des Steuergeräts notwendige Code vollständig im lesegeschützten OTP-Bereich des μC abzulegen statt diesen aus einem Master-Code und einem Sub-Code zusammenzusetzen.

Das Steuergerät kann im Sinne dieser Erfindung beispielsweise ein Motorsteuergerät, ein Getriebesteuergerät oder auch ein Kombiinstrument darstellen.

Mit einem erfindungsgemäßen Verfahren und dem erfindungsgemäßen Steuergerät können gegenüber herkömmlichen Steuergeräten eine große Anzahl von Vorteilen erzielt werden.

Mit dem erfindungsgemäßen Steuergerät kann auf zuverlässige Weise ein Austausch einzelner oder mehrerer Bausteine verhindert werden, da durch einen solchen Austausch die Funktion des Steuergeräts verhindert werden kann. Das Auslesen eines für die Funktion der Steuerung zwingend erforderlichen Teils des Programms bzw. der Daten ist nicht möglich, wenn dieser Teil in dem lesegeschützten OTP-Bereich abgelegt ist. Damit kann eine Vervielfältigung der Software verhindert werden. Auch ist der Zugriff auf vertrauliche Daten über die Kontaktierung des Bausteins nicht möglich, wenn diese in dem lesegeschützten OTP-Bereich des μC abgelegt sind. Besonders sicher kann das Steuergerät vor Manipulationen geschützt werden, indem es nur in der Kombination von Master- und Sub-Code lauffähig ist. Eine Veränderung des im reprogrammierbaren, gegebenenfalls externen Speicher, z.B. Flash, abgelegten Sub-Codes führt ohne eine Anpassung des Mastercodes zu einem Steuergeräteausfall. Weiterhin können Daten, die beispielsweise auf einem E^{2}PROM abgelegt sind, steuergeräteindividuell verschlüsselt werden. Auch die Entschlüsselung solcher Daten kann von einer Kennung des Steuergeräts abhängig gemacht werden. Zusätzliche Sicherheit kann dadurch geschaffen werden, dass die Ver- und Entschlüsselung von dem Verbund der einzelnen Bausteine mit den dem μC bekannten ID's abhängig gemacht wird.

Zusammenfassend kann also festgestellt werden, dass durch das Speichern einer unveränderbaren Kennung der Speicherbausteine eines Steuergeräts die Manipulation von Steuergeräten, wie beispielsweise Chip-Tuning bei Motorsteuergeräten, zuverlässig vermieden werden kann.

IP 4537
Pz

Patentansprüche

1. Fahrzeug-Steuergerät, das in einem Fahrzeug montiert ist und das zumindest einen ursprünglichen Mikrorechner (μC) und zumindest einen ursprünglichen Speicherbaustein (2, 3) beinhaltet, **dadurch gekennzeichnet, dass**
der ursprüngliche Speicherbaustein (2, 3) zumindest eine, spezifische Kennung (ID) aufweist und der ursprüngliche Mikrorechner (μC) zumindest einen Bereich (11) aufweist, in dem mindestens diese eine spezifische Kennung (ID) des ursprünglichen Speicherbausteins (2,3) abgelegt ist.

2. Fahrzeug-Steuergerät nach Patentanspruch 1, **dadurch gekennzeichnet, dass**
der Mikrorechner-Bereich (11), in dem die spezifische Kennung (ID) des mindestens einen Speicherbausteins (2, 3) abgelegt ist, nur einmalig beschreibbar ist.

3. Fahrzeug-Steuergerät nach einem der Ansprüche 1 oder 2 **dadurch gekennzeichnet, dass**
das Fahrzeug-Steuergerät (1) eine Authentifizierungseinheit (12) zur Authentifizierung der mit dem Mikrorechner (μC) verbundenen Speicherbausteine (2, 3) aufweist.

4. Fahrzeug-Steuergerät nach Anspruch 3, **dadurch gekennzeichnet, dass**
die Authentifizierungseinheit (12) durch ein Programm gebildet wird, das auf dem Mikrorechner (μC) abgelegt ist und das Programm dem Vergleich der Kennungen (ID) des ursprünglichen Speicherbausteins (2, 3) mit der Kennung (ID) des aktuellen Speicherbausteins (2, 3) dient.

5. Fahrzeug-Steuergerät nach Anspruch 3, **dadurch gekennzeichnet, dass**
die Authentifizierungseinheit (12) durch ein Programm gebildet wird, das auf dem Mikrorechner (μC) abgelegt ist und der Verschlüsselung von Daten dient, wobei das Programm zur Verschlüsselung von Daten oder Programmen auf mindestens eine der in dem Mikrorechner (μC) gespeicherten Kennungen (ID) eines ursprünglichen Speicherbausteins (2, 3) zugreift.

6. Fahrzeug-Steuergerät nach einem der vorangegangenen Ansprüche, **dadurch gekennzeichnet, dass**
mindestens einer der Speicherbausteine (2, 3) in dem Mikrorechner (μC) integriert ist.

7. Fahrzeug-Steuergerät nach Anspruch 1, **dadurch gekennzeichnet, dass**
das Fahrzeug-Steuergerät ein Motorsteuergerät ist.

8. Fahrzeug-Steuergerät nach Anspruch 1, **dadurch gekennzeichnet, dass**
das Fahrzeug-Steuergerät ein Getriebesteuergerät ist.

Translation

PCT/EP2003/008024

525229

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference IP 4537 PCT	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP2003/008024	International filing date (*day/month/year*) 23 July 2003 (23.07.2003)	Priority date (*day/month/year*) 21 August 2002 (21.08.2002)
International Patent Classification (IPC) or national classification and IPC G06F 1/00		
Applicant AUDI AG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 11 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
17 March 2004 (17.03.2004)	20 December 2004 (20.12.2004)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP2003/008024

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages _____, as originally filed
pages _____, filed with the demand
pages 1-9, filed with the letter of 15 November 2004 (15.11.2004)

☒ the claims:

pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages 1-8, filed with the letter of 15 November 2004 (15.11.2004)

☒ the drawings:

pages 1/4-4/4, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-8	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-8	NO
Industrial applicability (IA)	Claims	1-8	YES
	Claims		NO

2. Citations and explanations

Reference is made to the following document:

D1: EP-A-1 197 826 (TOKYO SHIBAURA ELECTRIC CO)
17 April 2002 (2002-04-17)

1. The present application does not meet the requirements of PCT Article 33(1) because the subject matter of claim 1 does not involve an inventive step within the meaning of PCT Article 33(3).

1.1 The indicated technical problem addressed by the present application is that of providing a motor vehicle control device, in which a memory chip cannot be replaced and the data and the code held on the memory chip modified without affecting the functional ability of the motor vehicle control device (see the description, page 1, last paragraph to page 2, paragraph 1).

1.2 However, the fact that the present application pertains to a motor vehicle control device cannot be considered a special technical feature, does not contribute to solving the above-indicated problem

and therefore in no way restricts the field of application.

1.3 Therefore, in order to evaluate the closest prior art, a person skilled in the art would consider all documents pertaining to the securing of electronic devices against unauthorized interference with memory chips.

1.4 D1 discloses a process for protecting such a device (in this case a portable memory card). The problem addressed by the invention described in D1 is that of providing a process for protecting such a device from interference, in which undesired memory chip modifications are prevented. For example, not even the owner can replace a memory chip without affecting the functional ability of the device. Further, two identifiers are compared with each other and, in addition, an encoding process that uses a component-specific identifier of a second component of the device as the key initially encodes data that are later stored in a reversible memory chip.

D1 is considered to represent the closest prior art in relation to the subject matter of claim 1.

1.5 In particular, D1 discloses (the references in parentheses are to this document) a secured electronic device (see column 1, lines 18-24) comprising a microcomputer and a memory chip (see column 3, lines 42-45; column 4, lines 16-19; figure 17), wherein the memory chip has a specific identifier ("memory 4 is certified by use of the *certification key* ... unalterably stored in the memory

4") and the microcomputer has an area in which this specific identifier of the memory chip is stored ("certification key unalterably stored in the internal memory 3b", see the first embodiment, column 4, lines 26-38).

1.6 The subject matter of claim 1 thus differs from that of D1 in that the present application pertains to a motor vehicle control device. However, this feature cannot be considered a special technical feature, does not contribute to solving the above-indicated problem and therefore in no way restricts the field of application. Claim 1 therefore does not involve an inventive step within the meaning of PCT Article 33(3).

2. Dependent claims 2-8 do not contain any features which, in combination with the features of any claim to which they refer back, meet the PCT requirements for inventive step.

2.1 **Claims 2, 3 and 4.** The subject matter of claims 2, 3 and 4 is likewise known from D1, since the microcomputer area (ROM memory portion) in which the identifier of the memory chip is stored is a write-once area, the device has an authentication unit for authenticating the memory chip connected to the microcomputer and the authentication unit is formed of a program that serves to compare the identifiers.

2.2 **Claim 5.** The subject matter of claim 5 is also known from D1 because the authentication unit is formed of a program that serves to encode data, wherein the program accesses an identifier stored in the microcomputer (see the third and fourth embodiments:

column 7, lines 34-41 and 49-53; column 8, lines 30-41; figures 14 and 17).

2.3 **Claims 6, 7 and 8.** Claims 6, 7 and 8 describe only such features as a person skilled in the art would consider to be routine design measures for solving the problem of interest.